

AMENDED IN ASSEMBLY MARCH 17, 2016

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL

No. 2720

Introduced by Assembly Member Chau

February 19, 2016

An act to add Section 11549.41 to the Government Code, relating to state government technology.

LEGISLATIVE COUNSEL'S DIGEST

AB 2720, as amended, Chau. State government: Office of Information Security: cybersecurity vulnerability reporting.

Existing law establishes the Office of Information Security in the Department of Technology, the purpose of which is to ensure the confidentiality, integrity, and availability of state systems and applications.

This bill would authorize the office to establish a Cybersecurity Vulnerability Reporting Reward Program for the purpose of soliciting eligible individuals to identify and report previously unknown vulnerabilities in state computer networks and making a monetary award for an eligible report, subject to appropriation of sufficient funds by the Legislature. The bill would require the office to develop policies, standards, and procedures for the administration of the program, including eligibility and award criteria. The bill would specify that the minimum award shall be \$100, and the maximum award shall be \$5,000. The bill would prohibit an individual from receiving an award unless he or she, among other things, has not attempted to access another person's data, or otherwise has not engaged in any unlawful, disruptive, or damaging activity in the course of investigating the existence of the suspected vulnerability and is not a state employee or contractor, or

the spouse or immediate family member of a state employee or contractor.

~~Existing law establishes the Office of Information Security in the Department of Technology, the purpose of which is to ensure the confidentiality, integrity, and availability of state systems and applications.~~

~~This bill would authorize the office to establish a Cybersecurity Vulnerability Reporting Reward Program for the purpose of soliciting eligible individuals to identify and report previously unknown vulnerabilities in state computer networks and making a monetary award for an eligible report, subject to appropriation of sufficient funds by the Legislature.~~

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: no.

The people of the State of California do enact as follows:

- 1 SECTION 1. Section 11549.41 is added to the Government
- 2 Code, immediately following Section 11549.4, to read:
- 3 11549.41. (a) The office, subject to appropriation of sufficient
- 4 funds by the Legislature, may establish a Cybersecurity
- 5 Vulnerability Reporting Reward Program for the purpose of
- 6 soliciting eligible individuals to identify and report previously
- 7 unknown vulnerabilities in state computer networks and making
- 8 a monetary award for an eligible report.
- 9 (b) The chief shall have sole discretion, subject to this section,
- 10 to determine the eligibility of a reported vulnerability and of the
- 11 individual reporting the vulnerability, and whether to make an
- 12 award, and, if so, in what amount.
- 13 (c) The office shall develop policies, standards, and procedures
- 14 for the administration of the program, including eligibility and
- 15 award criteria, subject to the following requirements:
- 16 (1) The policies, standards, and procedures shall specify all of
- 17 the following:
- 18 (A) That the priority of the program is to identify vulnerabilities
- 19 in state networks that could compromise the integrity of user data,
- 20 circumvent the privacy protections in use to protect user data, or
- 21 enable unauthorized access to state networks or infrastructure.
- 22 (B) Which state agencies and departments are included in the
- 23 program.

1 (C) *Qualifying and nonqualifying vulnerabilities.*

2 (D) *That the minimum award for a qualifying vulnerability shall*
3 *be one hundred dollars (\$100), and the maximum award shall be*
4 *five thousand dollars (\$5,000).*

5 (E) *That the determination of the amount of an award made*
6 *within the range established by subparagraph (D) shall be solely*
7 *at the discretion of the chief, based upon the sensitivity of the*
8 *reported vulnerability, the specificity of the report, and any other*
9 *factor that the chief may deem to be relevant.*

10 (2) *A vulnerability report may be eligible for an award only if*
11 *both of the following requirements are met:*

12 (A) *The vulnerability was not previously known or reported to*
13 *the office.*

14 (B) *The report contained all necessary information and is in*
15 *the required format, as specified by the office.*

16 (3) *An individual may receive an award for submitting an*
17 *eligible vulnerability report only if all of the following requirements*
18 *are met:*

19 (A) *He or she has not attempted to access another person's*
20 *data, or otherwise has not engaged in any unlawful, disruptive,*
21 *or damaging activity in the course of investigating the existence*
22 *of the suspected vulnerability.*

23 (B) *He or she is not on any federal sanctions list, or located in*
24 *a country that is on any federal sanctions list.*

25 (C) *He or she submits a vulnerability report that includes, but*
26 *is not limited to, a description of the vulnerability, the specific*
27 *risks involved, and at least one valid description of the*
28 *circumstances under which the vulnerability could be exploited.*

29 (D) *He or she is not a state employee or contractor, or the*
30 *spouse or immediate family member of a state employee or*
31 *contractor.*

32 (E) *He or she does not knowingly make any false, fictitious, or*
33 *fraudulent statements or representations to the office when*
34 *submitting information under this section, or knowingly include*
35 *any false, fictitious, or fraudulent writing, document, statement,*
36 *or entry therein.*

37 (d) *Nothing in this section shall be construed to authorize or*
38 *immunize the violation of law or agreement in any way, or to*
39 *otherwise disrupt, damage, or compromise the data or systems of*
40 *another person.*

1 (e) Any reward that remains unclaimed after a period of 12
2 months shall be deposited into the General Fund.

3 ~~SECTION 1. Section 11549.41 is added to the Government~~
4 ~~Code, to read:~~

5 ~~11549.41. The office, subject to appropriation of sufficient~~
6 ~~funds by the Legislature, is authorized to establish a Cybersecurity~~
7 ~~Vulnerability Reporting Reward Program for the purpose of~~
8 ~~soliciting eligible individuals to identify and report previously~~
9 ~~unknown vulnerabilities in state computer networks and making~~
10 ~~a monetary award for an eligible report.~~